PICUS | JUVENTUS OFFICIAL EXPOSURE VALIDATION PARTNER

CASE STUDY

How Juventus Strengthens Cyber Defense with Picus Security

Founded in 1897 and based in Turin, Juventus Football Club is one of the most successful and historic football clubs in the world. Competing in Serie A, the club has built a global reputation for excellence, winning numerous domestic league titles and major international honors, including the UEFA Champions League. Known for its iconic black-and-white colors and the motto “Fino alla Fine” (“Until the End”), Juventus plays its home matches at the Allianz Stadium and reaches hundreds of millions of supporters worldwide through its sporting achievements, cultural impact, and commitment to innovation both on and off the pitch.

About Juventus

Industry: Professional Sports / Entertainment

Headquarters: Italy

Number of Employees: 250

Products:

- Picus Security Validation Platform
- Picus Exposure Validation

Challenges:

- Manual security audits providing only periodic snapshots
- Complex attack surface across stadium, training, hospitality, and medical facilities
- Large volumes of sensitive personal, financial, and medical data
- Limited visibility into control effectiveness
- High effort and cost of traditional assessments

Results:

- Real-time insight into security posture
- Centralized exposure validation across all key facilities and systems
- Safe simulation of real-world attacks
- Clear understanding of control effectiveness
- Reduced time and cost through continuous automated validation

Protecting a Global Football Brand: How Juventus Strengthens Cyber Defense with Picus Security

As one of the world’s most recognized football clubs, Juventus F.C. operates in a highly visible and complex digital environment. With millions of global fans and intense match-day attention, protecting sensitive operational and personal data is essential.

To strengthen its cybersecurity posture and move beyond periodic security assessments, Juventus partnered with Picus Security to continuously validate its defenses and ensure its systems are ready to respond to evolving threats.

The Challenge: Securing a Global Sports Enterprise

Juventus manages multiple facilities and technology environments that support the club's operations, including Allianz Stadium, the training center, J Hotel, and J Medical, the club's medical center. These locations generate and store significant amounts of sensitive data, including personal, medical, and financial information.

According to Mirko Rinaldini, Head of Information and Communication Technology (ICT) for Juventus Football Club, protecting these environments requires constant vigilance.

> ***"With global fans constantly paying attention and match-day pressure, Juventus isn't a typical organization. We have to protect our digital environment and our facilities, such as Allianz Stadium, the training center, J Hotel, and J Medical, our medical center. This is challenging because of the amount of data—personal, medical, and financial—that we own and that requires different kinds of protection in our daily operations and during match days."*** **Rinaldini said.**

The club must also manage multiple external partners while ensuring that its cybersecurity defenses remain effective against modern threats. ***"We have to manage several external providers, and we have to be sure that our security posture is ready to face internal and external threats,"*** he explained.

Traditionally, Juventus relied on standard cybersecurity practices such as audits, vulnerability assessments, and penetration testing. While valuable, these methods provided only periodic insight into the organization's security posture.

> ***"With a traditional approach like audits, vulnerability assessments, and penetration tests, we have only a snapshot of the situation, and you need to put a lot of effort and cost into these activities two or three times per year," Rinaldini noted.***

The Solution: Continuous Exposure Validation

To address these limitations, Juventus adopted Picus Security's exposure validation approach. This allows the organization to simulate real-world cyberattacks and evaluate how its defenses respond in real time.

> ***"With Picus and its exposure validation approach, we are able to check the security posture of our organization and our security systems in real time, whenever we need," Rinaldini said.***

Exposure validation enables the security team to safely simulate attacks and analyze how their defenses react under realistic conditions.

> ***"Exposure validation means we are able to simulate external attacks and check if and how our defenses react," he added.***

This approach gives Juventus continuous visibility into its cybersecurity readiness and allows the team to validate the effectiveness of their defensive tools whenever needed.

Why Juventus Chose Picus Security

Juventus selected Picus Security because of its innovative approach to security validation and its ability to provide actionable insights.

> ***"We chose to partner with Picus because of their innovative approach that suggests how we can improve our defenses,"*** **Rinaldini said.**

The Juventus team also values the collaborative nature of the partnership.

> ***"Their platform is constantly evolving, and they listen to our feedback,"*** **he added.**

Results:

By implementing Picus Security's exposure validation platform, Juventus has moved from periodic security testing to continuous validation of its cybersecurity defenses.

This shift allows the organization to better understand its security posture, respond more quickly to potential risks and maintain strong protection for the club's operations and sensitive data.

For a global sports organization operating under constant attention, this level of visibility and validation is essential.

Watch Mirko Rinaldini, Head of ICT at Juventus Football Club **talk about his experience utilizing picus**

WATCH NOW ▶

picussecurity.com

Experience Picus *in Action*

GET A DEMO

Gartner Peer Insights Customers' Choice 2025

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 30 October 2025

WINTER 2026 Leader

4.9/5.0

#1 Solution Provider*

Breach and Attack Simulation

*G2, Breach and Attack Simulation (BAS) Solutions, Winter Grid Report, 3 December 2025